AIR WAR COLLEGE

AIR UNIVERSITY

INTEGRATING AIR, SPACE, AND CYBERSPACE:

TOWARDS CROSS-DOMAIN OPERATIONS

by

Matthew C. Harris, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

16 February 2011

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Biography

Lieutenant Colonel Matthew Harris is a United States Air Force Cyber Operations Officer. Colonel Harris received his commission in 1990 as a Distinguished Graduate of the Reserve Officer Training Corps (ROTC) at the University of Oklahoma, where he earned a Bachelor of Business Administration degree in Management Information Systems. He has also earned a Master of Business Administration at the University of Nebraska in 1998 and a Master of Military Operational at the United States Air Force Air Command and Staff College in 2003. Colonel Harris has held positions as squadron commander, flight commander, and executive officer at base level, as well as positions at the United States Strategic Command, United States Pacific Command and the Pentagon. He was the Deputy Commander, 375th Mission Support Group at Scott Air Force Base, Illinois immediately prior to attending Air War College.

Introduction

In December 2005, the United States Air Force (USAF) released a new mission statement, which concluded with the phrase "...to fly and fight in Air, Space and Cyberspace;" following a 2008 update it is now "...to fly, fight, and win...in air, space, and cyberspace." Yet, three years later, it is not clear we have a well defined construct for "fighting" and "winning" in the cyber domain as the mission statement would require. Historically, our cyber efforts have focused on defending our systems and networks as they perform vital, but supporting, tasks for operations in the "natural" domains (air, land, maritime, and space.) However, as information technology becomes increasingly pervasive, inexpensive and capable, the USAF must clearly articulate the "ways" cyber power can be used as a "means" to achieve operational and strategic "ends." It is unlikely that any future conflict will be fought and won completely in the cyber domain and equally unlikely that cyber power can "go it alone" and achieve major military or political objectives, except perhaps in the most unusual circumstances. Therefore USAF cyber power must be fully integrated with, not separated from, air and space power and used in concert with actions in the natural domain to achieve our ends.

In the 1950's, the USAF's strategy for countering the Soviet threat with air power and nuclear weapons offered just two choices: 1) keep the nuclear forces on the sidelines in a constant state of readiness, or 2) use them in an all-out nuclear war if deterrence failed. Beyond this all or nothing strategy, it was unclear how USAF airpower contributed to the nation's overall defense strategy and provided operational value in between the two extremes, and therefore its usefulness was greatly limited in the eyes of policy makers. The underlying problem 60 years ago is not dissimilar to one we face with cyber power today: how to fully integrate what is possible technically into a useable capability that can achieve strategic and operational objectives across a wide range of operations.

Beginning in 1953, the Air War College at Maxwell Air Force Base conducted "Project Control," a year-long study to determine if air power used in conjunction with other elements of national power could control Soviet behavior without the U.S. building a large conventional deterrent force or resorting to all-out nuclear war. While Project Control's conclusions were not fully embraced by senior leaders in the Air Force and administration, several concepts were later used during the Cold War. More relevant to our current challenge with cyberspace however, the Project Control study provides a model for the USAF to follow in developing a construct that moves cyber from a supporting role to a useful power projection capability. This seems particularly attractive as defense budgets are likely to decrease further or remain fairly stagnant for the foreseeable future.

Thesis: To create tangible and useful power projection capabilities in the cyber domain, the USAF should conduct a Project Control-like study to develop a cross-domain approach that integrates the active use of cyber power with air and space power, to create operational and strategic effects across all domains that can be used in concert with other elements of national power (diplomatic, informational, and economic) to achieve national objectives.

The Need for Cross-Domain Operations

> *Thus, cyberspace operations should be tightly integrated with capabilities of the air and space domains into a cohesive whole, commanded by an Airman who takes a broader view of war, unconstrained by geographic boundaries*.[1]

Information technology rapidly advanced over the last half century but the concept of the man-made cyber domain being a separate environment in which we can have a "presence," take action, and achieve ends, has only recently gained traction. The U.S. military is highly dependent upon interconnected information systems for intelligence, planning, command and control and administrative functions. Potential adversaries have taken notice and strive to penetrate, exploit, and possibly disrupt these systems.   Logically, this threat has heavily weighed our efforts towards defense of our systems and maintaining our ability to effectively operate in the cyber domain. While the U.S. as a nation relies on cyberspace, our near-peer adversaries and even non-state actor are becoming increasingly cyber-dependant as well. This presents a new opportunity to shift our focus from simply defending our own cyber systems to actively using the cyber domain to our advantage. Simply, it offers us additional means and ways to achieve a wide variety of ends to further our military objectives and national interests.

I do not to suggest cyber can consistently achieve major or enduring military objectives on its own, however. Integration is vital. Just as ground, air, space and maritime forces operate in environments and situations where their effects are more or less useful, cyber power will also be more or less relevant in each situation. And when efforts are combined, the integrated effects can be greater than simply the sum of each domain on its own. This highlights the need to consider how cyber power can, and more importantly when it should, be used in a variety of situations, along with actions in the other domains. Recent USAF cyber doctrine recognizes the need for integration, yet little is provided on how this should be done. Creating an approach for actively using cyber power is best done in deliberate fashion, not in the "heat of battle," and I believe should be done as an effort to develop a cross-domain operations concept that fully integrates action across the USAF domain "triad" - air, space and cyberspace. The USAF's efforts during the early years of the Cold War provide a useful model of how to transform a new capability into new operational concepts.

New Technologies Drive New Operating Concepts

Historically, the introduction of new military technologies have often outpaced the doctrine and operational concepts needed to maximize their effectiveness. For example, despite continual evolution of tactics throughout World War II, long-range bombers remained an enabler for surface warfare and were used in a supporting role to prepare the battlefield in advance of ground or maritime forces. While strategic bombing offered the potential for shortening the war and minimizing Allied casualties, it was always assumed that victory required invasion of Germany and Japan. Nazi Germany surrendered only after Allied ground forces descended on Berlin, despite the prolonged strategic bombing campaign against the German industrial centers and population centers. Similarly, Japan endured massive destruction from B-29 fire bombing missions and the U.S. planned for a full-scale invasion of the Japanese islands, until Japan finally surrendered following the atomic bombing of Hiroshima and Nagasaki in August of 1945. While historians still debate the relative importance of the atomic bombings versus Soviet's declaration of war to Japan's surrender, to some strategists Japan's surrender suggested that air power, in the form of a nuclear weapon armed strategic bomber, had now become decisive.

Following the Korean War in the early 1950's, the U.S. began to fully rely on nuclear weapons as its primary means of defense and airpower truly began to step out from the shadows of ground and naval power. This new ability to project overwhelming power over long distances with a relatively small force allowed the U.S. to remain powerful militarily without having to maintain a large conventional force. Rather than just a bigger bomb to be used in <u>support</u> of ground and maritime forces, nuclear weapons could be used <u>instead</u> of large conventional forces, and at much less expense. This conclusion seemed particularly attractive as the Soviet Union, with her capacity to maintain a massive conventional force, began to exert pressure on the U.S.

during the late 1940's and early 1950's. Our position as the sole nuclear power and desire to avoid a conventional force build-up to match the Soviet's resulted in the doctrine of nuclear deterrence by threat of "massive retaliation." Simply, our doctrine was to respond to any military provocation with nuclear weapons, which theoretically would deter any potential aggressor. Unfortunately, it created several problems: the all-or-nothing approach limited U.S. policymaker's ability to respond to anything short of an all-out war for national survival, it required a willingness to launch a preemptive first strike, and it didn't really provide "cheap" security as it simply shifted the inevitable escalation of force buildup from conventional to nuclear forces as the Soviets had tested their first nuclear weapon in 1949.

The Origins of Project Control

The problems created by downsizing conventional forces and focusing on nuclear capabilities became apparent when we entered the Korean War ill equipped and poorly prepared. Korea cleanly split the seam between the nuclear capabilities we had and conventional capabilities we lacked. Nuclear weapons were irrelevant in a "police action" in another country, and we had to revert to conventional warfare using WWII-era technology and tactics. Instead of learning a critical lesson, Korea was viewed as an aberration and the U.S. remained committed to massive retaliation with nuclear weapons as the guiding defense strategy throughout the 1950's.

Each service tried to increase its role in the country's nuclear strategy and share of the defense budget in President Eisenhower's "New Look", nuclear focused defense policy.[2] For the USAF, that meant tactical aircraft became just another means to deliver smaller nuclear weapons, and emphasis was placed on more numerous and more capable strategic bombers. Though the Navy considered the concept of strategic bombing with nuclear weapons "both costly and immoral"[3] they planned to build an aircraft carrier that could carry strategic bomber sized aircraft with nuclear weapons. The Army even reorganized, equipped, and trained to fight on the "atomic battlefield" in an effort to remain relevant. But the dilemma demonstrated in Korea should have been clear: massive retaliation with nuclear weapons was a "one size fits all" strategy that left the U.S. military (and the USAF in particular) without a scalable and useable force to achieve strategic and operational objectives for anything less than all out nuclear war.

However, this problem was not lost to all. During a briefing in the late 1940's on the strategic bombing campaign to be used in the event of war with the USSR, observed that U.S. political goals regarding Russia could not be obtained through nuclear bombing.[4] While specific to the Soviets, this insight on nuclear weapon's inability to achieve national objectives had broader implications. Noting this disconnect, USAF Colonel Raymond S. Sleeper began to consider how to use air power to control Soviet behavior through ways other than just bombing them into submission with nuclear weapons. This led to a year-long effort at the USAF's Air War College to further develop his "air control" concept.

Air Control versus Deterrence through Massive Retaliation

The massive retaliation doctrine was an extreme form of deterrence, itself a subset of coercive theory, the basics of which is simply communicating to another party that if you do "x" to me, I will do "y" to you. Theoretically, if the other party fears "y" enough, they will not do "x." With massive retaliation, U.S. doctrine stated that if attacked in any way we would respond with a massive nuclear attack and any aggressor would face certain destruction. While simple, to be effective this approach required that potential enemies had to believe the U.S. would actually respond to virtually any aggression with nuclear weapons. Additionally, they had to believe that the U.S. had the ability to effectively respond with sufficient number of nuclear weapons to defeat them. Further, they had to believe that our nuclear posture was purely defensive in nature and that the U.S. wouldn't be the aggressor and attack unprovoked. While only a partial list, the above issues were the key problems the doctrine faced as a viable policy.

In contrast to deterrence, the concept of "controlling" another implied an active effort in determining their behavior, which Colonel Sleeper believed would be more effective for dealing with the Soviet's. "Air control" meant the use of air power, in conjunction with other efforts, to actively demonstrate both U.S. will and ability to act. Where deterrence was somewhat passive, control was clearly more active. The concept was successfully used in a more limited capacity by the British in Iraq and other areas of their Empire in the 1920's and 1930's at significantly less cost than if large numbers of ground forces had been employed. The British experience drove Colonel Sleeper's interest in the concept of "control by air and other means," or "CAOM," and his belief that it was worth in-depth study for the Soviet problem.

The Project Control Study

The Project Control study took place at Maxwell Air Force Base, Alabama in 1953 and into 1954. The team was led by Colonel Sleeper, who was assigned to the Air War College at the time, and was comprised of a wide mix of military officers and civilian professionals from Air University and other locations, as well as academic consultants hired specifically for the study. Air War College, Air Command and Staff School and other Air University students at Maxwell AFB participated, and over the course of the project well over one hundred individuals were involved. Expertise ranged from intelligence specialists in Japanese, German, Soviet and U.S. military capabilities to those with strategic and operational planning experience. The project was divided into three main efforts: 1) a historical analysis of how the CAOM concept might have been applied to Japan prior to and during WWII; 2) a similar analysis of Germany; and 3) an in depth analysis how Soviet behavior might be modified through CAOM.[5] In addition, towards the end of the project the team was asked, and quickly produced, a study focused on emerging problems in Indochina.[6] As this was a prelude to our later involvement in Vietnam, it is unfortunate that the team's work was overshadowed by the results of the Soviet study as in retrospect the CAOM concept had much more to offer in non-nuclear scenarios.

Control by Air and Other Means

As a concept, CAOM is a fairly simple. The premise was that air power should be the main effort, rather than supporting the overall strategy as it had been in WWII.[7] Colonel Sleeper believed Korea did offer one positive lesson, as the U.S. used airpower and "a strategy of forcing the enemy to accept terms through increasing pressure," which he believed provided a "good example of the requirement to harmonize the use of air power to the (sic) obtaining of U.S. political objectives."[8] Air power, through air control, could give the USAF a way to present scalable options that could directly support national objectives and offered a better solution than massive retaliation. Although air-centric, the concept explicitly required use of other military capabilities and national power elements as well in an integrated fashion.

The Project Control team identified five basic requirements and three distinct phases for CAOM implementation (see the Appendix for further detail). I believe it is worth noting here that the requirements of Capability, Intelligence, Objective, Communications and Control Structure are relevant in any domain you wish to influence or control an adversary's behavior, be it one of the natural domains, or the cyber domain. Additionally, CAOM would be applied through three distinct phases, Persuasion, Pressure, and Administration. The team used these requirements and phases as a framework for retrospective analysis of Japan and Germany prior to and during WWII, and a forward looking analysis and development of the Soviet CAOM strategy.

Project Control Historical Studies

The team concluded that COAM could have effectively achieved most national objectives for both Japan and Germany earlier and at less cost than occurred during WWII. Regarding Japan, they determined that peace terms could have been reached 13-16 months sooner, but with the important caveat that the terms would have to recognize the interests of Japan[9] and would not require Japan's "unconditional surrender," which was a key U.S. demand at the time. The war with Germany could similarly have ended as much as 18 months earlier if the Allies had negotiated with the Nazi regime, but again Germany's unconditional surrender could not be expected. The benefit in both cases was a quicker end to the fighting, with significantly less cost in lives and national treasure for all parties. However the team assumed a major concession on the Allies part that would have been virtually impossible to accept during the war. Politics demanded complete surrender of both Japan and Germany once the war began, yet CAOM didn't provide a clear way to achieve that objective.

The Soviet Study

The team concluded however that the Soviet Union could be controlled by a CAOM strategy, in concert with "strategic political warfare," which combined political and military means to discredit the prestige of the USSR's political and economic leadership.[10] The report argued that the U.S. should conduct a series of political pushes to reunify Germany and dissolve the Iron Curtain, as well as maintain pressure on China and other Soviet allies. Persuasive air actions included reconnaissance over flights of Russia, not only as a show of force but also as a collection effort against Soviet nuclear efforts, and a forward air patrol across the Arctic near the Russian border. While the team believed persuasion efforts alone would likely be successful in modifying Soviet behavior, it depended on the U.S. maintaining clear nuclear superiority and "use of this capability to avoid war and maintain peace through persuasion operations, or if necessary peripheral pressure operations."[11] If persuasion failed to achieve desired results, pressure would be increased through a first-strike with nuclear weapons against Soviet nuclear weapons sites, followed by armed reconnaissance actions to bring the USSR to agreeable terms. In additional to the use of nuclear weapons, success also relied upon regime change to a group able to effectively control the country and willing to work with the U.S; ostensibly the group most suited for this was the Russian military itself. [12] The administration phase of a "new Russia" would be conducted primarily through air patrols and "liaison forces" to assist the new regime.

Upon conclusion of the study Colonel Sleeper extensively briefed the results to senior leaders in the Air Force, Office of the Secretary of Defense, Joint Staff, State Department, and possibly even President Eisenhower. Not surprisingly, reviews were mixed. While the team's development and theoretical application of the CAOM concept provided a number of interesting and potentially useful insights, senior military and civilian leadership deemed it results regarding the Soviets too optimistic and clearly dangerous. Following the concept to conclusion required accepting that the U.S. might have to initiate a nuclear war with the Soviet's to force them to come to acceptable terms, yet starting what amounted to a <u>preventative</u> nuclear war was not in line with the U.S. national policy. The concept, as applied to the Soviets, simply pushed the national policy too far off course in an effort to match it with the capability air power and nuclear weapons provided. The Soviet persuasion phase was war gamed with "inconclusive results", and did not result in further war gaming or generate renewed interest in the project.[13]

Clearly, the application of the CAOM concept to the Soviet problem was flawed as, like the Japanese and German studies, it unrealistically assumed away critical political constraints.

Yet, as one author appropriately highlights, Colonel Sleeper's concept of applying pressure in an "active, dynamic" way was perhaps the central and most important theme of the project. The notion that airpower should primarily be a deterrent force standing by to retaliate was rejected; what was needed was an understanding of "how to effect a 'positive air strategy for a positive political offensive.'"[14] Indeed, the final report emphasized that "it should be made clear that the concept of CAOM does not wait for all-out war for its use. Neither does its use dictate that the war must be total."[15] Clearly, for Colonel Sleeper air power was a force to be used, not a capability in waiting. This theme, as well as the team approach Project Control used, can be carried forward to today as we consider the use of cyberpower.

Then and Now

While the domains, technologies, and political realities faced by the Project Control team and USAF strategists are different, there are similar challenges that make the approach useful when considering the cyber domain today. In both cases, an opportunity was 'created' by the introduction of new and rapidly advancing technologies, allowing the USAF to operate differently in emerging domains. Aircraft technology improved at a tremendous rate following WWII, as the jet engine and other developments improved speed, range, and combat capabilities of fighter, bomber, and reconnaissance aircraft. And although space was not a factor at the time of Project Control, Colonel Sleeper's team envisioned the development of reconnaissance satellites within a relatively short timeframe as a further extension of USAF capabilities that would be useful for CAOM. For our generation, the cyber domain has grown in size, speed of operation, and range of functions that can be performed at an even faster pace than airpower during the first half of the 20th century. With these opportunities come challenges, as such rapid advancements in what we could "technically do" and what we could "operationally do" in the air domain outpaced one another during Colonel Sleeper's time. The challenge we face in the cyber domain today is the same, only more so.

Both air and cyber powers offer the potential for far reaching effects, in terms of geographic distance and in the tactical, operational, and strategic levels of warfare. CAOM used air power to apply persuasion and pressure tactics (if needed) at specific locations across a wide area rather than invade an enemy with a large ground force to physically control the country. Further, these methods could be scaled up or down relatively easily and quickly either in number of targets hit and/or type of action taken, from intimidation by simply flying over a target all the way to actually using a nuclear weapon, depending on the desired effect. Similarly, the cyber domain offers great scalability in precision, as well as both "soft" and "hard" effects, and both air and cyber offer this potential at less cost when compared to actions in the land and maritime domains. Granted, you can only compare the effectiveness and cost of actions in situations where there is "common ground" in the operating domains, but when you have options to achieve the effect you need (such as shutting down a radar site), either air or cyber power will likely be more "cost effective" and timely than a surface operation. The challenge, however, is selecting the right action to achieve the desired effect, and not causing collateral and unanticipated damage in the process.

Finally, during the early years of the Cold War, it was difficult to obtain accurate intelligence on the Soviet's capabilities due to the large expanse of Soviet territory and closed society. Long-range reconnaissance aircraft and satellites eventually improved our collection capabilities, but accurate and timely information always remained a challenge. We face the same challenge in the cyber domain. Unlike much of the physical domain, the cyber domain cannot be directly observed in the traditional sense. The physical and logical dimensions of the domain are in constant flux, with systems and nodes continually coming on and off line. Unlike a runway, bridge or even the location of enemy forces, a critical cyber system/node identified and targeted for attack may ”instantly” be relocated logically on the network so the targeting information is no longer accurate. Enemy system vulnerabilities may get patched during maintenance, or “mirror” systems are kept in “hot” status so they can instantly come on line and replace failed systems, compounding the targeting problem and limiting the effects of an attack. Whether or not establishment of USCYBERCOM, and linking the NSA and Service cyber capabilities, will successfully address this issue remains to be seen. The flexibility offered by the cyber domain creates challenges knowing our adversaries capabilities which, while difficult to envision today given our intelligence capabilities in the physical domain, are not unlike those faced during the early years of the Cold War. In sum, the challenges posed by rapid technical advances, the wide range of possible effects and difficulties “knowing” our adversaries capabilities only strengthen the argument for a Project Control-like effort focused on cyber power integration.

The Way Forward: A Cross-domain Operations Construct

> *Since air, space and cyberspace are inextricably linked both operationally and technically, the potential exists to integrate capabilities across these domains to exponentially increase each other's power. This integration promises to give joint force commanders unrivaled global access, persistence, awareness and connectivity capabilities and to rapidly restore critical infrastructure via a cross-domain network-of-networks approach. The USAF will seek to develop cyber capabilities that complement those of other services and will explore the combination of cyber with other non-kinetic capabilities to achieve synergies*.[16]

Challenged to find the best way to use cyber power, the USAF could simply focus on the standalone capabilities and effects cyber can provide within its own domain, in isolation of other domains and capabilities. Clearly, however, this is not the best way forward, as the above quote suggests. Our senior leaders recognize the interdependence of air, space and cyberspace and the need for integrated efforts, not separate ones. However, the aperture needs to be broader than just further “systems integration,” more “jointness” and providing better ways to “support” the war fighter as the above could infer. We must strive to fully integrate our newest operating domain into our warfighting approach. We must develop a truly cross-domain operations construct that integrates the USAF triad of air, space, and cyberspace, rather than continue to use cyberpower as a supporting arm for actions in the natural domains. This means employing all three domains consistent with our mission statement, by developing a more balanced approach that employs cyber throughout the lifecycle of operations, from planning through execution. It may be that in many operations cyber remains primarily a supporting effort, but the point is to not assume away cyber power’s role at any point, just as air and space contributions shouldn’t be presupposed. Doing so however is easier said than done, in part due to a natural hesitancy to move from capabilities that are tangible, well understood and have proven track records, such as kinetic airpower, to a relatively new and unproven capability like cyberpower.

This is not a new situation, however. When the CAOM concept offered a new option for dealing with the Soviets, the USAF committed the time and resources necessary to study the problem in depth and further develop the concept into a new strategy. Though the project’s recommendations failed to be adopted by military and civilian policy makers, the study itself presents a useful example of how to take capabilities offered by relatively new technologies and integrate them with other well-understood means to develop a new approach to achieve our objectives. Following a similar approach and challenging a cross-functional team of experts to develop a strategy to achieve a rational set of national military objectives, fully integrating the “unknown” capabilities of cyberpower with the “known” capabilities in air and space and those in the surface domains, offers real value. Perhaps the most important aspect of the Project Control study was that it was done outside the “normal” planning process, away from day-to-day operational requirements, daily crises of staff work, and other distractions.[17] The singular focus allowed a fairly small group of experts (many whom were already resident at Air University) to develop, document, and advocate for a new defense strategy in little more than a years time.

Taking the Project Control approach a step further, as noted previously the CAOM requirements Colonel Sleeper's team identified are applicable regardless of domain. Modified to incorporate the cyber domain with the other physical domains, the requirements for cross-domain operations might reflect the following.

Capability	To balance the air, space, cyberspace "triad," further develop cyber capabilities that provide a range of effects & options integrated w/actions in physical domains, and all instruments of national power, to achieve desired objectives
Intelligence	Focus intelligence collection on: typical military/national capabilities & intentions, adversary military cyber capabilities, systems & intentions, and related/connected civilian systems to fully understand system & functional relationships
Objective	Military objective in sync w/national objectives, consistent with real capabilities and achievable effects; apply right capability in right domain for the mission
Communication	Communications w/adversary must be maintained; origin (attribution) & even effect of actions in the cyber domain may not be immediately apparent direct communication is needed
Control	State, non-state, & individual actors (particularly in cyber domain) are all potential adversaries; given not all actors in cyber domain will operate at the direction of a controlling authority, purely defensive operations will remain essential to cyberspace operations

Table 1. Cross-domain Operations Requirements

An application of the cross-domain requirement to a notional scenario is presented in Table A-3 of the appendix, and although a simple and certainly not definitive representation the intent is simply to show that approaching cyber inclusively with other domains, vice exclusive of them, offers considerably more means and ways to achieve our ends.

Recommendation and Conclusion

The level of expertise, effort and information needed to translate an overall concept, such as CAOM or cross-domain operations, into concrete actions requires the commitment of time and resources on the scale of the Project Control study. I believe it is an effort worth serious consideration. A team of experts in intelligence, operations planning, information operations and space systems, as well as individuals with relevant international relations expertise would be required specific to the scenarios to be studied, and as with Project Control an analysis of both historical and potential future adversaries across the range of military operations would be appropriate. While these types of studies do occur in our operational communities, there is value to doing this outside of our “normal” processes. What may result is a new cross-domain operations construct that enhances USAF and joint capabilities, increases our value to national policy makers, and provides new ways to achieve both military and national ends.

Appendix

Requirement	Description
Capability	Ability to control the air in the hostile area
Intelligence	Political, psychological, economic, and military intelligence
Objective	The objective of controlling the behavior of the hostile area, with feasible terms that will achieve the political objective
Communications	Continuous communication with the hostile or controlling groups/individuals; establish and maintain ability to transmit information, warnings, terms, and receive reactions and acceptances
Indigenous Control Structure	Organization that controls, or has the potential of controlling, the hostile nation and can accept and implement terms

Table A-1. Project Control CAOM Requirements

Phase	Description	Joint Ops Planning Phases
Persuasion	Show of force persuades hostile area to behave in acceptable manner	Ph 0-I, Shape & Deter
Pressure	Delivery of fire power by air forces	Ph II - III, Seize Init & Dominate
Administration	Follows acceptance of terms, may involve air policing of controlled area	Ph IV - V, Stabilize & Enable Civil Authority

Table A-2. Project Control CAOM Phases

	Capability	Intelligence	Objective	Communication	Control
Phase 0 - I (Persuade)	- Show of force in air/sea/land as permits; consider limited & temporary disruption of media & cyber access	- Space, air and cyber collection activities; assess capability & intent	- Demonstrate US interest & resolve	- Communicate resolve & acceptable behavior	- Identify controlling authority(ies) (CA), if any
	- Public & private diplomatic pressure	- Cyber focused on access/exploitation	- Reassure allies	- Hostile nature of enemy's actions	- Shape comms to CAs
	- Economic sanctions		- Intel prep of battlefield		
Phase II - III (Pressure)	- Cross domain power application; emphasize speed and simultaneous effects in multiple domains	- Continual BDA, ID new targets, assess enemy capability & intent to continue	- Gain and hold military advantage	- Communicate resolve and terms for ending hostilities	- Monitor and adjust if CA's change throughout engagement
	- Disrupt military C2, commercial comm capabilities				
	- Increased economic and diplomatic pressure				
Phase IV - V (Admin)	- Maintain physical and cyber presence	- Assess compliance with terms, capabilities & intent	- Monitor and demonstrate US resolve	- Communicate resolve and acceptable behavior	“
	- Public & private diplomatic pressure				

Table A-3. Notional Cross-Domain Operations Application & Phasing

Bibliography

Air Force Doctrine Document (AFDD) 3-12: *Cyberspace Operations.* 15 Jul 2010.

Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. Department of Defense Report. Washington D.C.: Office of the Secretary of Defense, 2010.

Bacevich, A. J. *The Pentomic Era: The US Army Between Korea and Vietnam*. Washington D.C. National Defense University Press: 1986.

Biddle, Tami D. "Handling the Soviet Threat: 'Project Control' and the Debate on American Strategy in the Early Cold War Years." *The Journal of Strategic Studies*, Vol 12, Number 3, (September 1989): 273-302.

The Concept of Control by Air and Other Means: Project Control Final Report, Call # K239.042-9, IRIS#479646, AFHRA, Maxwell AFB, AL. June 1954. Document is now declassified.

Dean, David J. "Project Control: Creative Strategic Thinking at Air University." *Air University Review*, July-August (1984).

Gagnon, George R. "Air Control: Strategy for a Smaller United States Air Force." Maxwell AFB, AL: Air War College, Air University, 1993: 17-28.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* (Fall 2010): 102-135.

Joint Publication (JP) 3-0. *Doctrine for Joint Operations.* 2001.

Kuehl, Daniel T., and Robert A. Miller. "Cyberspace and the "First Battle in 21st Century War." *Defense Horizons,* Number 68, (September 2009).

Lamb, Michael W. "Bytes: Weapons of Mass Disruption." Maxwell AFB, AL: Air War College, Air University, 2002.

Lewis, Andrew L. "The Revolt of the Admirals." Maxwell AFB, AL: Air Command and Staff College, Air University, April 1998.

Libicki, Martin. *Cyberdeterrence and Cyberwar.* Arlington, VA: RAND Corp., 2009.

Mueller, Karl, "The Essence of Coercive Air Power: A Primer for Military Strategists." *Air and Space Power Journal Chronicles,* (September 2001).

Office of the President of the United States. *Cyberspace Policy Review*. Washington D.C. 2009.

Schroeter, Robert C. "Dominating Networks in Cyberspace: It Isn't What It's Hacked Up To Be." Maxwell AFB, AL: Air Command and Staff College, Air University, 2008.

Stein, George. "Twenty-first Century Airpower: the Integrating Imperative." Maxwell AFB, AL: Air War College, Air University, 2010.

United States Air Force, Air Combat Command. *2010 Combat Air Force Strategic Plan*. Langley AFB, VA: ACC/A5, 2010.

United States Air Force, Air Force Space Command. *The United States Air Force Blueprint for Cyberspace.* Peterson AFB, CO, 2009.

United States Department of Defense. *The National Military Strategy of the United States of America*, 2011.Washington D.C.: Chairman of the Joint Chiefs of Staff, 8 February 2011.

End Notes

[1] AFDD 3-12, *Cyberspace Operations*, 14.

[2] Bacevich, *The Pentomic Era: The US Army Between Korea and Vietnam*, 15.

[3] Lewis, "The Revolt of the Admirals,"12.

[4] *The Concept of Control by Air and Other Means: Project Control Final Report*, 1.

[5] Biddle, "Handling the Soviet Threat: 'Project Control' and the Debate on American Strategy in the Early Cold War Years," 281.

[6] Dean, "Project Control: Creative Strategic Thinking at Air University," 5.

[7] *The Concept of Control by Air and Other Means: Project Control Final Report*, 9.

[8] *The Concept of Control by Air and Other Means: Project Control Final Report*, 7.

[9] *The Concept of Control by Air and Other Means: Project Control Final Report*, 55.

[10] Gagnon, "Air Control: Strategy for a Smaller United States Air Force," 21.

[11] *Concept of Control by Air and Other Means: Project Control Final Report*, 66.

[12] Gagnon, "Air Control: Strategy for a Smaller United States Air Force," 21.

[13] Biddle, "Handling the Soviet Threat: 'Project Control' and the Debate on American Strategy in the Early Cold War Years", 292-293.

[14] Biddle, "Handling the Soviet Threat: 'Project Control' and the Debate on American Strategy in the Early Cold War Years", 283.

[15] *Concept of Control by Air and Other Means: Project Control Final Report*, 61.

[16] United States Air Force, Air Force Space Command, *The United States Air Force Blueprint for Cyberspace*, 6.

[17] Dean, "Project Control: Creative Strategic Thinking at Air University," 8.